Angewandte diskrete Mathematik

Wintersemester 2008/2009
Barbara Baumeister
Jürgen Schütz

Freie Universität Berlin
Institut für Mathematik

Aufgabenblatt 11

Ausgabe: 13.1.2009

Abgabe: 20.1.2009

Aufgabe 41. — 4 Punkte

Cycling-Attacke: Sei (n, e) ein öffentlicher RSA-Schlüssel. Für einen Klartext $m \in \mathbb{Z}_n$ sei $c = m^e \bmod n$ der zugehörige Schlüsseltext.

a) Zeige, dass es ein $k \in \mathbb{N}$ gibt, für welches $m^{e^k} \equiv m \pmod{n}$ für alle $m \in \mathbb{Z}_n$ gilt.

b) Folgere, dass für ein solches k und alle $m \in \mathbb{Z}_n$ $c^{e^{k-1}} \equiv m \pmod{n}$ ist. Ist dies eine Bedrohung für RSA?

c) Sei $n = 493$ und $e = 3$. Bestimme das kleinste k, für das die Cycling-Attacke funktioniert.

Aufgabe 42. — 4 Punkte

Alice besitze den öffentlichen Schlüssel $(p, \alpha, \beta) = (107, 2, 80)$. Als Verifikation für eine ElGamal-Signatur gibt sie

$$v(x, u_1, u_2) = \text{wahr} \quad \Longleftrightarrow \quad 80^{u_1} u_1^{u_2} \equiv 2^x \pmod{107}$$

bekannt. Sie signiert die Nachricht x mit $(9, 93)$. Welche der folgenden Nachrichten $x = 10$, $x = 83$, $x = 17$ ist sicher nicht von Alice, also gefälscht?

Aufgabe 43. — 4 Punkte

Wie kann Oskar die Zufallszahl k bei der ElGamal-Signatur finden, wenn Alice das gleiche k zur Signatur zweier verschiedener Nachrichten benutzt?

Aufgabe 44. — 4+1 Punkte

Entwerfe einen polynomiellen Algorithmus, der bei Eingabe von natürlichen Zahlen c und e entscheidet, ob c eine e-te Potenz ist und gegebenenfalls die e-te Wurzel von c berechnet. Zeige, dass der Algorithmus tatsächlich polynomielle Laufzeit hat.

Zusatz: Implementiere den Algorithmus.